

(54) METHOD AND DEVICE FOR CONDUCTING TRUSTED REMOTE PAYMENT TRANSACTIONS

(75) Inventors: Gyan Prakash, Beaverton, OR (US); Selim Aissi, Beaverton, OR (US)

(73) Assignee: Intel Corporation, Santa Clara, CA (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 12/785,138

(22) Filed: May 21, 2010

(65) Prior Publication Data

US 2011/0289004 A1 Nov. 24, 2011

(51) Int. Cl.

G06Q 20/00 (2012.01)

H04L 29/06 (2006.01)

G06Q 20/32 (2012.01)

G06Q 20/20 (2012.01)

G06Q 20/38 (2012.01)

G06Q 20/40 (2012.01)

(Continued)

(52) U.S. Cl.

CPC ..... G06Q 20/32 (2013.01); G06Q 20/20 (2013.01); G06Q 20/206 (2013.01); G06Q 20/223 (2013.01); G06Q 20/325 (2013.01); G06Q 20/3223 (2013.01); G06Q 20/3278 (2013.01); G06Q 20/3823 (2013.01); G06Q 20/3829 (2013.01); G06Q 20/40 (2013.01); G06Q 20/425 (2013.01)

(58) Field of Classification Search

USPC ..... 705/64

See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS

5,319,542 A 6/1994 King, Jr. et al.

5,354,158 A 10/1994 Sheldon et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN 1591499 A 3/2005

CN 1591499 A 3/2005

(Continued)

OTHER PUBLICATIONS

“Near Field Communication”, Wikipedia, The Free Encyclopedia, retrieved on Apr. 2, 2011, Webpage available at: <[http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication)>.

(Continued)

Primary Examiner — Calvin L Hewitt, II

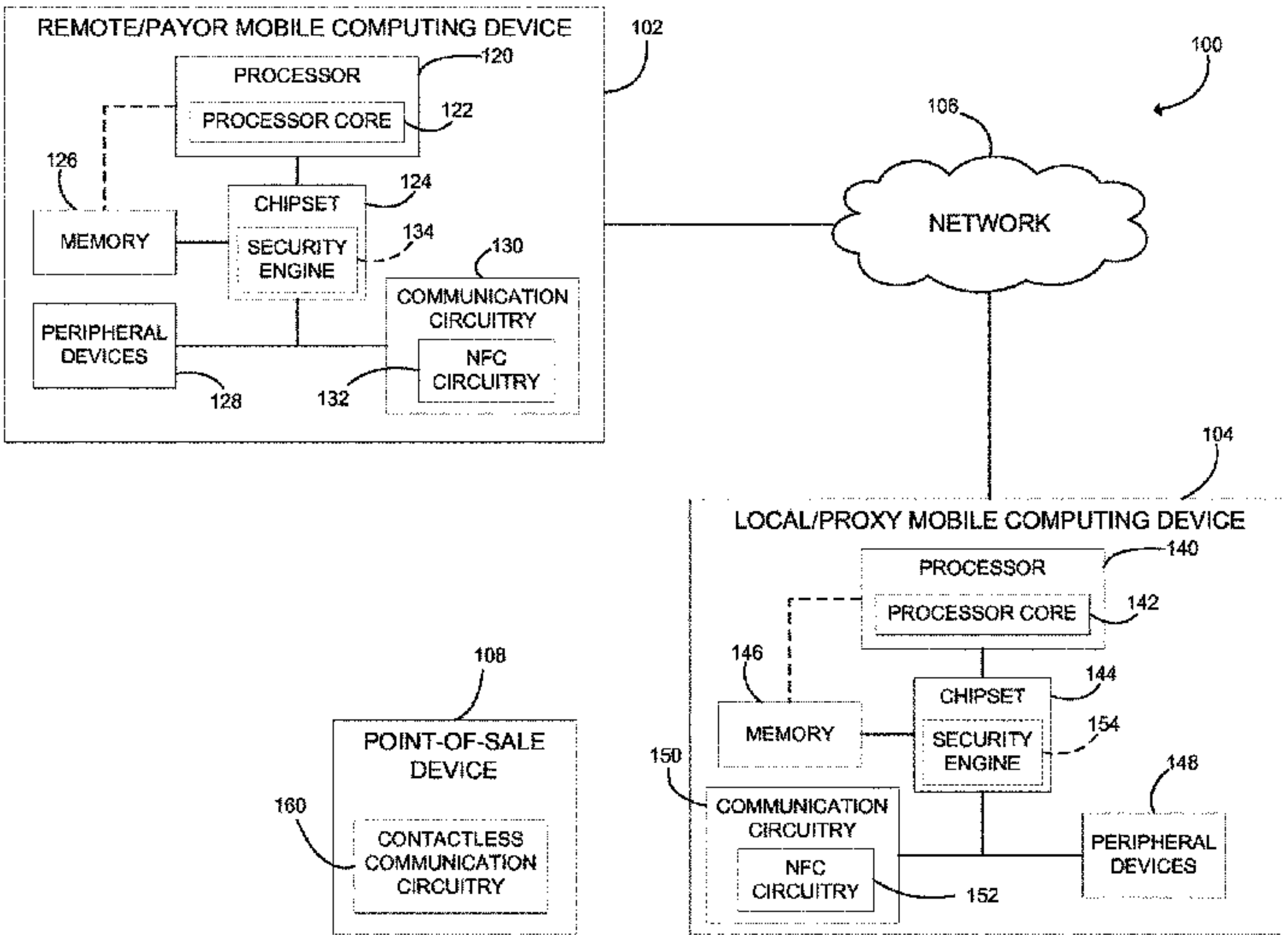
Assistant Examiner — Aaron McIntyre

(74) Attorney, Agent, or Firm — Barnes & Thornburg LLP

(57) ABSTRACT

A method, device, and system for conducting trusted payment transactions including establishing a trust relationship between a first mobile computing device and a second mobile computing device. The first mobile computing device may initiate a payment transaction with a point-of-sale device, communicate with the second mobile communication device to retrieve payment information from the second mobile communication device, and complete the payment transaction with the point-of-sale device using the payment information. The second mobile computing device is configured to verify the user and identity of the first mobile computing device prior to providing the payment information. Communications between the mobile computing devices may be encrypted using pre-determined encryption techniques.

16 Claims, 4 Drawing Sheets





(51) **Int. Cl.**  
**G06Q 20/42** (2012.01)  
**G06Q 20/22** (2012.01)

(56) **References Cited**

WO	2009039419	A1	3/2009
WO	2009060393	A	5/2009
WO	2009060393	A2	5/2009
WO	2010019353	A2	2/2010
WO	2011146678	A2	11/2011
WO	2011146678	A3	11/2011

## U.S. PATENT DOCUMENTS

5,402,336	A	3/1995	Spiegelhoff et al.	
6,880,761	B1	4/2005	Ritter et al.	
7,003,495	B1 *	2/2006	Burger et al.	705/50
7,127,236	B2	10/2006	Khan et al.	
7,434,723	B1 *	10/2008	White et al.	235/375
7,494,067	B1 *	2/2009	Zhu	235/492
2001/0029496	A1	10/2001	Otto et al.	
2002/0165831	A1	11/2002	Horn et al.	
2002/0174030	A1 *	11/2002	Praisner et al.	705/26
2003/0046289	A1	3/2003	Balasubramanian et al.	
2003/0055735	A1 *	3/2003	Cameron et al.	705/26
2003/0071115	A1	4/2003	Horn et al.	
2004/0029569	A1 *	2/2004	Khan et al.	455/414.1
2005/0068178	A1 *	3/2005	Lee et al.	340/569
2005/0156026	A1 *	7/2005	Ghosh et al.	235/380
2007/0022058	A1	1/2007	Labrou et al.	
2007/0055632	A1	3/2007	Hogl	
2007/0055635	A1	3/2007	Kanapur et al.	
2007/0116292	A1	5/2007	Kurita et al.	
2007/0244750	A1	10/2007	Grannan et al.	
2007/0255662	A1	11/2007	Tumminaro	
2007/0265984	A1 *	11/2007	Santhana	705/65
2008/0022101	A1	1/2008	Sung et al.	
2008/0046362	A1	2/2008	Easterly	
2008/0167961	A1	7/2008	Wentker et al.	
2008/0208743	A1 *	8/2008	Arthur et al.	705/41
2008/0222711	A1 *	9/2008	Michaelis	726/7
2008/0313079	A1	12/2008	Van Bosch et al.	
2009/0070263	A1	3/2009	Davis et al.	
2009/0119181	A1	5/2009	Pratt et al.	
2009/0132813	A1	5/2009	Schibuk	
2009/0143104	A1 *	6/2009	Loh et al.	455/558
2009/0222383	A1	9/2009	Tato et al.	
2009/0222659	A1	9/2009	Miyabayashi et al.	
2009/0233579	A1 *	9/2009	Castell et al.	455/411
2009/0281945	A1 *	11/2009	Shakkarwar	705/40
2010/0030695	A1 *	2/2010	Chen et al.	705/67
2010/0041368	A1	2/2010	Kumar	
2010/0043056	A1	2/2010	Ganapathy	
2010/0114731	A1	5/2010	Kingston et al.	
2010/0145850	A1	6/2010	Nagai et al.	
2010/0146607	A1	6/2010	Piepenbrink et al.	
2010/0250436	A1 *	9/2010	Loevenguth et al.	705/44
2010/0260388	A1 *	10/2010	Garrett et al.	382/124
2011/0131627	A1 *	6/2011	Abendroth et al.	726/1
2011/0140841	A1 *	6/2011	Bona et al.	340/5.83

## FOREIGN PATENT DOCUMENTS

CN	101527911	A	9/2009
CN	101527911	A	9/2009
CN	101656960	A	2/2010
DE	10310527	A	9/2004
DE	10310527	A1	9/2004
EP	2182493	A1	5/2010
JP	2002-189971	A	7/2002
JP	2004110307	A	4/2004
JP	2004-258739	A	9/2004
JP	2006-209453	A	8/2006
JP	2008-269062	A	11/2008
JP	2011-530957	A	12/2011
KR	2006-0103796		10/2006
KR	2006-0103796	A	10/2006
KR	2009-0121026		11/2009
KR	10-2009-0122968	A	12/2009
WO	9011572	A	10/1990
WO	9428497	A	12/1994
WO	9952066	A1	10/1999
WO	2005086593	A2	9/2005

## OTHER PUBLICATIONS

“Digital Wallet”, Wikipedia, The Free Encyclopedia, retrieved on Apr. 2, 2011, Webpage available at: <[http://en.wikipedia.org/wiki/Digital\\_wallet](http://en.wikipedia.org/wiki/Digital_wallet)>.

International Search Report and Written Opinion received for PCT/US2011/037086, mailed Feb. 9, 2012, 10 pages.

Official Communication received for Chinese Application No. 201110130193.9, mailed Apr. 2, 2014, 6 pages of Chinese Office Action and 13 pages of unofficial English translation.

Official Communication received for Russian Application No. 2012155628, mailed Feb. 13, 2014, 3 pages.

Office Action received for Korean Patent Application No. 2011-0048043, mailed on Sep. 30, 2013, 5 pages of Office Action including 2 pages of unofficial English translation.

Search Report received for European Application No. 11250498.0, mailed on Jun. 11, 2013, 5 pages.

Official Communication received for European Application No. 11250498.0, mailed on Jun. 24, 2013, 6 pages.

Office Action received for Korean Patent App. No. 10-2011-0048043, mailed Aug. 28, 2012, 3 pages of Korean Office Action and 1 page of unofficial English translation.

Result of Consultation issued by the European Patent Office, European Patent Application No. 11 250 498.0-1958, Sep. 25, 2014, 8 pages.

Appeal Decision issued by the European Patent Office, European Patent Application No. 96115736.9, Nov. 27, 2003, 11 pages.

International Preliminary Report on Patentability received for PCT Application No. PCT/US2011/037086, mailed on Dec. 6, 2012, 6 pages.

Official Communication received for European Patent Application No. 11250498.0, mailed on Feb. 12, 2014, 8 pages.

Arnall, “Thoughts on Nokia’s NFC developments,” The Touch Project, May 7, 2008, XP055098485, 10 pages.

Office Action received for Chinese Patent Application No. 201110130193.9, mailed on Jan. 31, 2013, 4 pages of Chinese Office Action and 5 pages of unofficial English translation.

Office Action received for Korean Patent Application No. 2011-0048043, mailed on Mar. 29, 2013, 4 pages of Korean Office Action and 4 pages of unofficial English translation.

Office Action received for Chinese Patent Application No. 201110130193.9, mailed on Jul. 18, 2013, 24 pages of Office Action including 15 pages of unofficial English translation.

Office Action received for Chinese Patent Application No. 201110130193.9, mailed on Aug. 14, 2012, 8 pages of Office Action including 5 pages of unofficial English translation.

Office Action received for Japanese Patent Application No. 2011-110368, mailed on Apr. 2, 2013, 4 pages of Japanese Office Action and 5 pages of unofficial English translation.

Decision of Rejection and English Translation for Chinese Application No. 201110130193.9, dated Apr. 2, 2014, 19 pages.

Summons to Attend Oral Proceedings for European Application No. 11250498.0-1958/2388744, dated Dec. 2, 2014, 8 pages.

Timo, “Thoughts on Nokia’s NFC developments,” Touch, May 7, 2008, 10 pages.

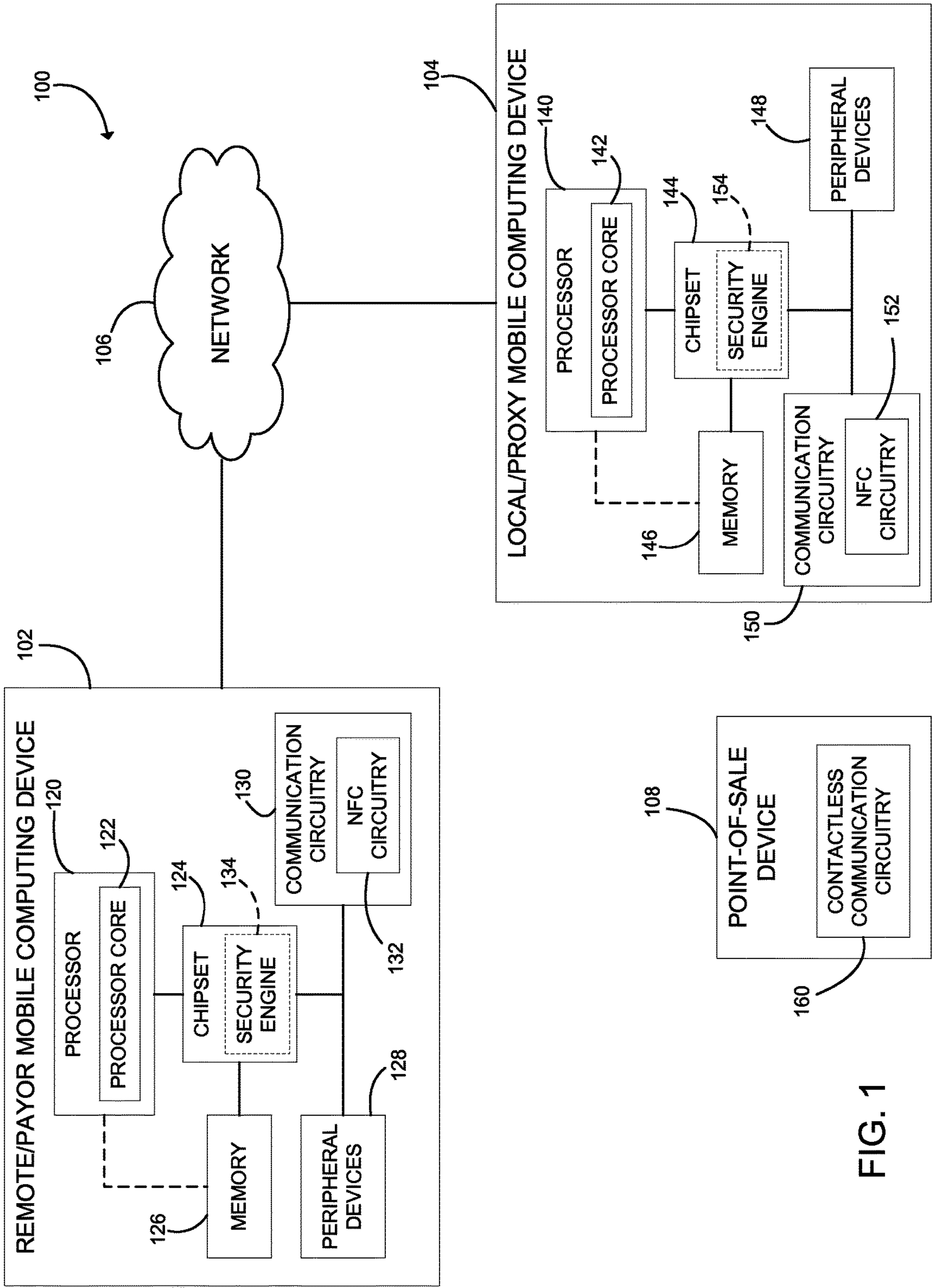
Office Action and English Translation for Korean Patent Application No. 2011-0048043, dated Apr. 28, 2015, 9 pages.

Decision to Refuse for European Patent Application No. 11250498.0-1958, dated Jan. 27, 2015, 23 pages.

Notice of Preliminary Rejection and English Translation for Korean Patent Application No. 2013-0131115, dated Sep. 5, 2016, 9 pages.

Decision of Reexamination for Chinese Application No. 201110130193.9, dated Mar. 29, 2016, 23 pages.

\* cited by examiner



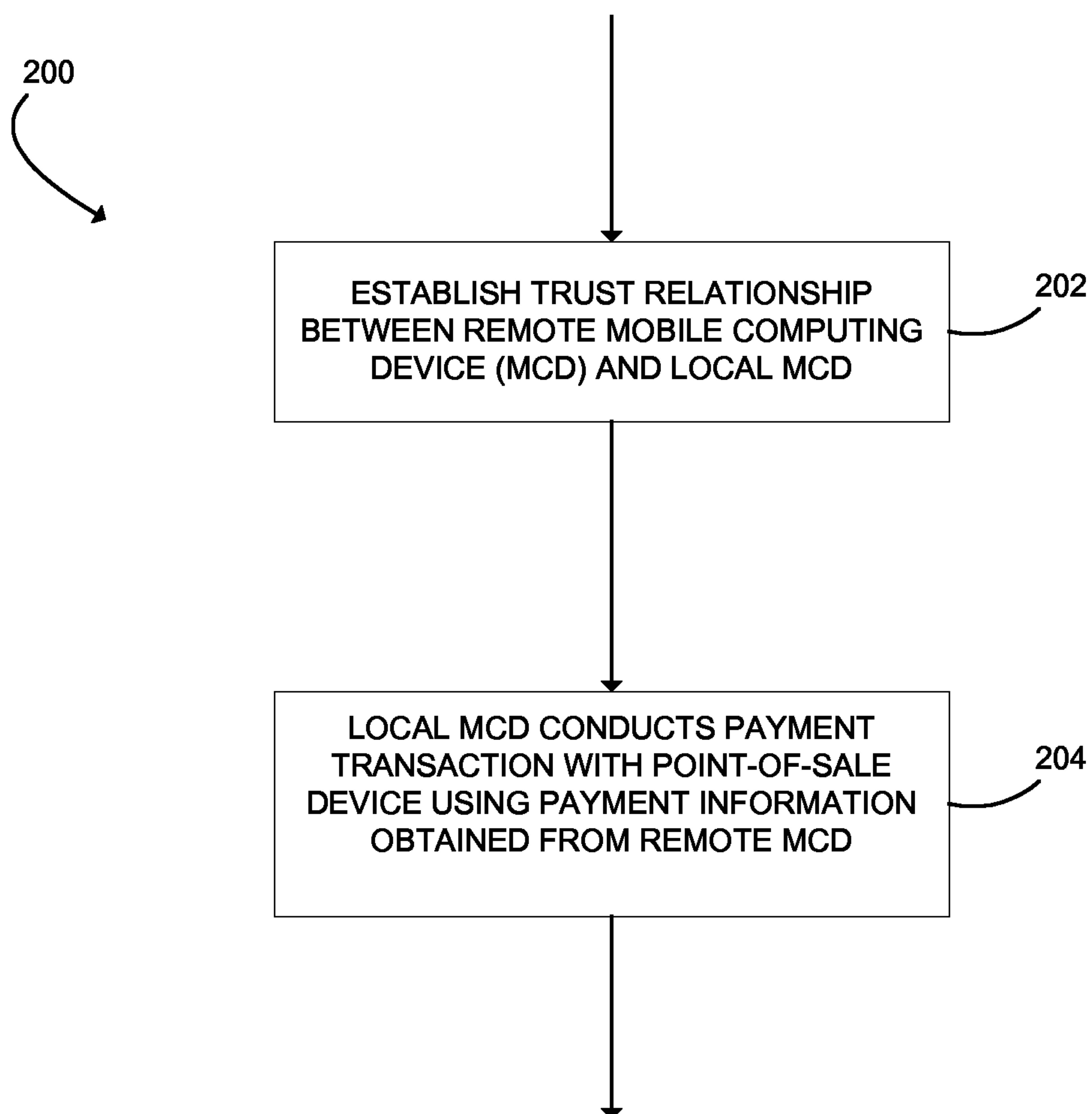


FIG. 2



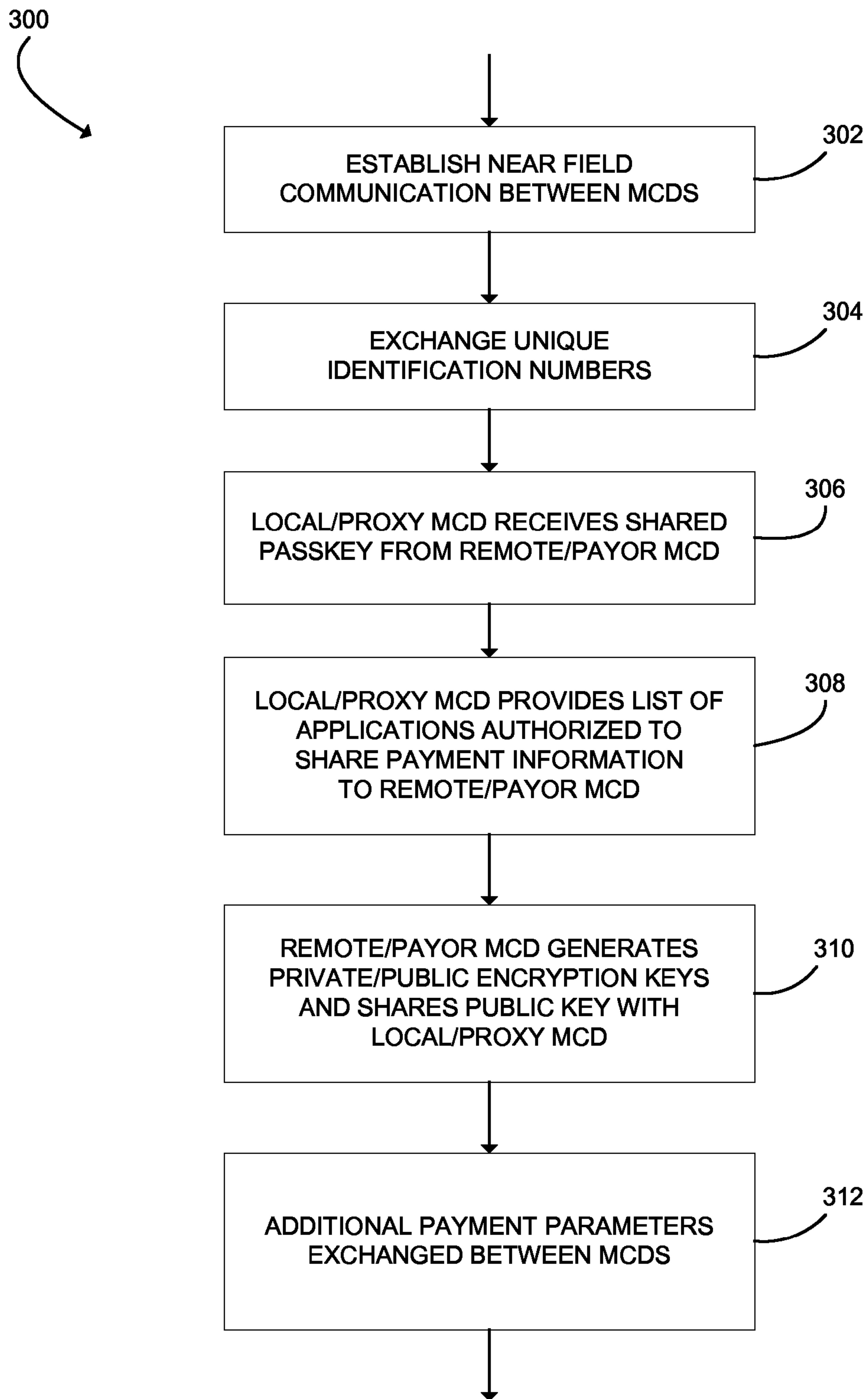


FIG. 3

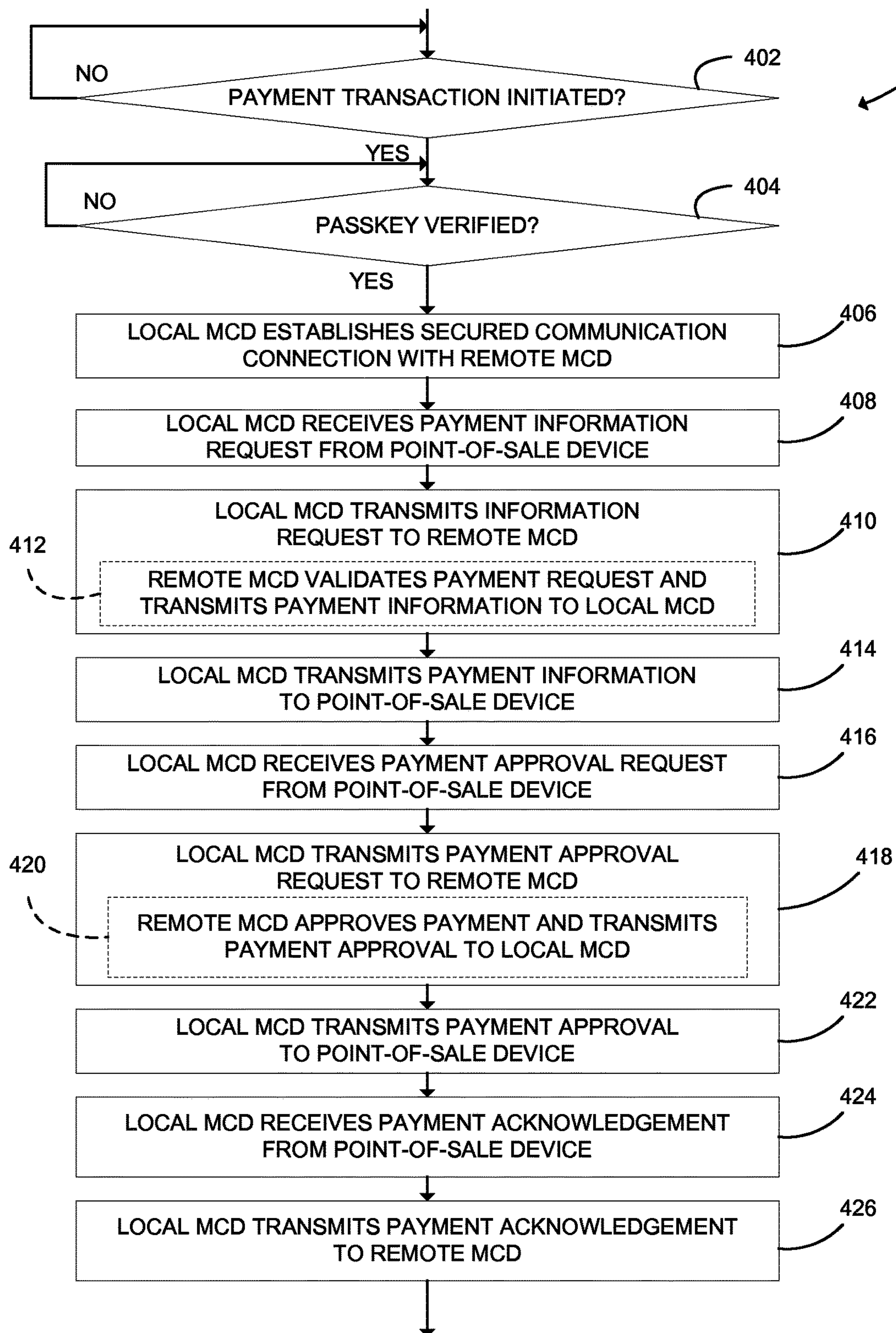


FIG. 4



## 1

# METHOD AND DEVICE FOR CONDUCTING TRUSTED REMOTE PAYMENT TRANSACTIONS

## BACKGROUND

Digital wallets (also known as “e-wallets” or “e-credit card”) and other electronic-based personal payment systems allow users to conduct electronic purchases and payment transactions without the necessity of physical credit/charge cards or other standard payment mediums (e.g., personal check). Digital wallets are typically embodied as software and associated hardware (e.g., a smartphone, personal digital assistant, a computer, etc.) on which the user’s account information is maintained. Some digital wallets may aggregate multiple credit/charge accounts of the user thereby allowing the user to carry a single electronic device while having access to the multiple credit and charge accounts.

Digital wallets may be used to complete transactions with pre-configured point-of-sale devices. Typically, such point-of-sale devices communicate with the digital wallet using contactless communication. Because the digital wallet is integrally associated with the electronic hardware (e.g., the smartphone) of the user, the smartphone or other electronic device must be physically present and local to the point-of-sale device to complete the payment transaction. As such, the owner of the digital wallet is typically unable to extend use of his or her credit/charge account to another, remote individual (e.g., parent to child) or otherwise authorize the payment of a purchase conducted remotely by another individual.

## BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

FIG. 1 is a simplified block diagram of one embodiment of a system for conducting trusted, remote payment transactions using mobile computing devices;

FIG. 2 is a simplified flow diagram of one embodiment of a method for conducting trusted payment transactions using the system of FIG. 1;

FIG. 3 is a simplified flow diagram of one embodiment of a method for establishing a trusted relationship between the mobile computing devices of FIG. 1; and

FIG. 4 is a simplified flow diagram of one embodiment of a method for conducting a payment transaction with a point-of-sale device using the mobile computing devices of FIG. 1.

## DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention

## 2

is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment”, “an embodiment”, “an example embodiment”, etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions stored on a tangible, machine-readable medium, which may be read and executed by one or more processors. A tangible, machine-readable medium may include any tangible mechanism for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a tangible, machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; and others.

Referring now to FIG. 1, a system 100 for conducting trusted payment transactions includes a remote or payer mobile computing device 102 and a local or proxy mobile computing device 104. In use, as discussed in more detail below, the local mobile computing device 104 acts as a proxy for the remote mobile computing device 102 in payment transactions with a point-of-sale device 108. To do so, the local mobile computing device 104 initiates a payment transaction with the point-of-sale device 108. During the payment transaction, the point-of-sale device 108 may request payment information from the local mobile computing device 104 to complete the payment transaction. In response to such a payment request, the local mobile computing device 104 is configured to communicate with the remote mobile computing device 102 over a network 106 to receive payment information from the device 102, which may be located remotely from the local mobile computing device 104 and the point-of-sale device 108. Because the mobile computing devices 102, 104 have a pre-established trust relationship, such communication may be encrypted or otherwise secured.



After the local mobile computing device **104** receives the payment information from the remote mobile computing device **102**, the mobile computing device **104** completes the payment transaction with the point-of-sale device **108** using the payment information. In this way, a user of the remote/ 5 payer mobile computing device **102** may authorize use of their payment information (e.g., credit account or charge account information) to a user of the local mobile computing device **104** without being physically present at the point-of-sale device **108**. For example, a parent may be the user of the payer mobile computing device **102** and a child of the parent may be the user of the proxy mobile computing device **104**. In such embodiments, the parent may remotely authorize, using the payer mobile computing device **102**, payment transactions conducted by the child using the proxy mobile computing device **104**.

Although only one remote/payer mobile computing device **102**, one local/proxy mobile computing device **104**, one network **106**, and one point-of-sale device **108** are illustratively shown in FIG. 1, the system **100** may include any number of mobile computing devices **102**, mobile computing devices **104**, networks **106**, and point-of-sale devices **108** of similar or dissimilar architecture. For example, the remote computing device **102** may be configured to communicate with multiple local mobile computing devices **104** to allow each device **104** to conduct payment transactions with one or more point-of-sale devices **108** using the payment information provided by the remote/payer mobile computing device **102**.

The remote mobile computing device **102** may be embodied as any type of mobile computing device capable of performing the functions described herein. For example, the remote computing device **102** may be embodied as a cellular phone, a smart phone, a mobile internet device, a handheld computer, a laptop computer, a personal digital assistant, a telephony device, or other portable computing device. In the illustrative embodiment of FIG. 1, the remote mobile computing device **102** includes a processor **120**, a chipset **124**, a memory **126**, one or more peripheral devices **128**, and communication circuitry **130**. In some embodiments, several of the foregoing components may be incorporated on a motherboard of the mobile computing device **102**, while other components may be communicatively coupled to the motherboard via, for example, a peripheral port. Furthermore, it should be appreciated that the mobile computing device **102** may include other components, sub-components, and devices commonly found in a computer and/or computing device, which are not illustrated in FIG. 1 for clarity of the description.

The processor **120** of the remote mobile computing device **102** may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like. The processor **120** is illustratively embodied as a single core processor having a processor core **122**. However, in other embodiments, the processor **120** may be embodied as a multi-core processor having multiple processor cores **122**. Additionally, the remote mobile computing device **102** may include additional processors **120** having one or more processor cores **122**.

The chipset **124** of the remote mobile computing device **102** may include a memory controller hub (MCH or “north-bridge”), an input/output controller hub (ICH or “south-bridge”), and a firmware device. The firmware device of the chipset **124** may be embodied as a memory device for storing Basic Input/Output System (BIOS) data and/or instructions and/or other information (e.g., a BIOS driver

used during booting of the mobile computing device **102**). However, in other embodiments, chipsets having other configurations may be used. For example, in some embodiments, the chipset **124** may be embodied as a platform controller hub (PCH). In such embodiments, the memory controller hub (MCH) may be incorporated in or otherwise associated with the processor **120**, and the processor **120** may communicate directly with the memory **126** (as shown by the hashed line in FIG. 1).

In some embodiments, the chipset **124** may include a security engine **134**. The security engine **134** may be embodied as hardware and/or firmware configured to perform security, encryption, and/or authentication functions as described in more detail below. For example, the security engine **134** may be embodied as or otherwise include an out-of-band processor, a trusted platform module (TPM), and/or other security enhancing hardware and/or associated software modules. As discussed in more detail below, the security engine **134** cooperates with a corresponding security engine **154** of the local mobile computing device **104** to establish a trusted relationship between the mobile computing devices **102, 104**.

The processor **120** is communicatively coupled to the chipset **124** via a number of signal paths. These signal paths (and other signal paths illustrated in FIG. 1) may be embodied as any type of signal paths capable of facilitating communication between the components of the mobile computing device **102**. For example, the signal paths may be embodied as any number of wires, cables, light guides, printed circuit board traces, via, bus, intervening devices, and/or the like.

The memory **126** of the remote mobile computing device **102** may be embodied as one or more memory devices or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), flash memory devices, and/or other volatile memory devices. The memory **126** is communicatively coupled to the chipset **124** via a number of signal paths. Although only a single memory device **126** is illustrated in FIG. 1, in other embodiments, the mobile computing device **102** may include additional memory devices. Various data and software may be stored in the memory device **126**. For example, one or more operating systems, applications, programs, libraries, and drivers that make up the software stack executed by the processor **120** may reside in memory **126** during execution. Furthermore, software and data stored in memory **126** may be swapped between the memory **126** and a data storage device of the peripheral devices **128** as part of memory management operations.

The peripheral devices **128** of the remote mobile computing device **102** may include any number of peripheral or interface devices. For example, the peripheral devices **128** may include a display, a keyboard, a mouse, one or more data storage devices such as an internal or external hard drive, and/or other peripheral devices. The particular devices included in the peripheral devices **128** may depend upon, for example, the intended use of the remote mobile computing device **102**. The peripheral devices **128** are communicatively coupled to the chipset **124** via a number of signal paths thereby allowing the chipset **124** and/or processor **120** to receive inputs from and send outputs to the peripheral devices **128**.

The communication circuitry **130** of the remote mobile computing device **102** may be embodied as any number of



5

devices and circuitry for enabling communications between the remote/payer mobile computing device **102** and the local/proxy mobile computing device **104** over the network **106**. The network **106** may be embodied as any number of various wired and/or wireless telecommunication networks. For example, the network **106** may be embodied as or otherwise include one or more cellular networks, telephone networks, local or wide area networks publicly available global networks (e.g., the Internet), or any combination thereof. For example, in one embodiment, the network **106** is embodied as or otherwise includes a Global System for Mobile Communications (GSM) cellular network. Furthermore, the network **106** may include any number of additional devices to facilitate communication between the mobile computing devices **102**, **104** such as routers, switches, intervening computers, and/or the like. The mobile computing devices **102**, **104** may use any suitable communication protocol to communicate with each other over the network **106** depending on, for example, the particular type of network(s) **106**.

The communication circuitry **130** is also communicatively coupled to the chipset **124** via a number of signal paths. The communication circuitry **130** may include one or more wired and/or wireless network interfaces to facilitate communications over the wired and/or wireless portions of the network **106**. In some embodiments, the communication circuitry **130** may include Near Field Communications (NFC) circuitry **132**. The NFC circuitry **132** may be embodied as relatively short-ranged, high frequency wireless communication circuitry, which may be incorporated in other circuitry of the communication circuitry **130** or separate therefrom. For example, in some embodiments, the effective communication range of the NFC circuitry **132** is no greater than about ten centimeters. The relatively short communication range of the NFC circuitry **132** allows validation of the physical presence of another communication device (e.g., the local/proxy mobile computing device **104**) when using the NFC circuitry **132** to communicate. Additionally, the NFC circuitry **132** allows the remote/payer mobile computing device **102** to conduct contactless communication with the local/proxy mobile computing device **104** and other contactless communication-enabled devices (e.g., the point-of-sale device **108**).

The local/proxy mobile computing device **104** may be substantially similar to the remote/payer mobile computing device **102** and may be embodied as any type of mobile computing device capable of performing the functions described herein. For example, similar to the remote mobile computing device **102**, the local mobile computing device **104** may be embodied as a cellular phone, a smart phone, a mobile internet device, a handheld computer, a laptop computer, a personal digital assistant, a telephony device, or other portable computing device. In the illustrative embodiment of FIG. 1, the local mobile computing device **104** includes a processor **140** having one or more processor cores **142**, a chipset **144** including a security engine **154**, a memory **146**, one or more peripheral devices **148**, and communication circuitry **150** including NFC circuitry **152**. The components of the illustrative local mobile computing device **104** are substantially similar, although not necessarily identical, to the corresponding components of the remote mobile computing device **102**. As such, the above-provided description of the processor **120**, the processor core(s) **122**, the chipset **124**, the memory **126**, the peripheral devices **128**, the communication circuitry **130**, the NFC circuitry **132**, and the security engine **134** of the remote/payer mobile computing device **102** is equally applicable to, respectively, of

6

the processor **140**, the processor core(s) **142**, the chipset **144**, the memory **146**, the peripheral devices **148**, the communication circuitry **150**, the NFC circuitry **152**, and the security engine **154** of the local/proxy mobile computing device **104** and is not repeated herein for clarity of the description.

In use, as discussed above, the local/proxy mobile computing device **104** may communicate with the remote/payer mobile computing device **102** directly via the NFC circuitry **132**, **152** and/or over the network **106**. Additionally, the local/proxy mobile computing device **104** may communicate with one or more point-of-sale devices **108** via the NFC circuitry **152** to conduct payment transactions. Such payment transactions may be embodied as any type of transaction in which the point-of-sale device **108** requests payment from the local mobile computing device **104** for services or products delivered by the point-of-sale device **108** or a device or entity associated with the point-of-sale device **108**. As such, the point-of-sale device **108** may be embodied as any device configured to communicate with mobile computing devices to request and receive electronic payments. To do so, the point-of-sale device **108** includes a contactless communication circuitry **160**, which may be embodied as near field communication circuitry configured to communicate with the NFC circuitry **152** of the local mobile computing device **104**. Of course, the point-of-sale device **108** may include other circuitry and devices depending on, for example, the type and use of the point-of-sale device **108**. For example, the point-of-sale device **108** may include a processor, memory, data storage device, monitor, keypad or other data entry device, printer, and/or other devices commonly found in point-of-sale devices.

As discussed above, the local mobile computing device **104** may be used to initiate a payment transaction with the point-of-sale device **108** and complete the payment transaction using payment information received from the remote/payer mobile computing device **102**. To do so, the local mobile computing device **104** communicates payment requests to and receives the payment information from the remote mobile computing device **102** using secured communications. The payment information may be embodied as any type of information required by the point-of-sale device **108** to complete the payment transaction. For example, the payment information may be embodied as account information of the user or owner of the remote/payer mobile computing device **102** such as credit card account information, charge card account information, bank account information, or other account information that may be used to effect payment of a debit. Such payment information may also include account validation information such as an account password, an account passkey, identification numbers, and/or the like.

Referring to FIG. 2, one illustrative embodiment of a method **200** for conducting trusted payment transactions using the system **100** of FIG. 1 begins with block **202**. In block **202**, a trust relationship is established between the mobile computing devices **102**, **104**. Any suitable methodology for establishing a trusted relationship between the devices **102**, **104** may be used in block **202**. In some embodiments, the NFC circuitry **132**, **152** of the devices **102**, **104** are used to initially establish the trust relationship by verifying physical presence of the local/proxy mobile computing device **104** relative to the remote/payer mobile computing device **102**. The trust relationship may be established for both the local mobile computing device **104** and the user of the local mobile computing device **104** with respect to the remote/payer mobile computing device **102**. For example, a password or passkey may be generated,



which must be entered on the local mobile computing device **104** before the remote mobile computing device **102** will send the payment information to thereby ensure the proper user is using the local mobile computing device **104**.

One illustrative embodiment of a method **300** for establishing a trust relationship between the mobile computing devices **102**, **104** is illustrated in FIG. 3. The method **300** begins with block **302** in which a near field communication is established between the mobile computing devices **102**, **104**. To do so, the devices **102**, **104** may be positioned near each other (e.g., within ten centimeters or in physical contact) and the NFC circuitry **132**, **152** of the devices **102**, **104** may be operated to establish the near field communication. By requiring establishment of near field communication, the physical presence of the local/proxy mobile computing device **104** relative to the remote/payer mobile computing device **102** is ensured. In this way, the identity of the local/proxy mobile computing device **104** to be trusted by the remote/payer mobile computing device **102** is validated.

In block **304**, the mobile computing device **102**, **104** exchange unique identification numbers. The unique identification numbers may be embodied as any type of numerical/alpha-numerical number that uniquely identifies the respective device **102**, **104**. For example, in one embodiment, the mobile computing device **102**, **104** exchange International Mobile Equipment Identify (IMEI) numbers in block **304**. The unique identification numbers may be used to validate the identity of the devices **102**, **104** during subsequent communications as described below.

In block **306**, the local/proxy mobile computing device **104** receives a shared passkey from the remote/payer mobile computing device **102**. The shared passkey may be generated by the remote/payer mobile computing device **102** or by a user of the device **102** or device **104**. The shared passkey is used to verify the identity of the person using the local/proxy mobile computing device **104**. For example, before communicating with the remote mobile computing device **102** to request the payment information, the user of the local mobile computing device **104** may be prompted to enter the shared passkey, thereby verifying that the authorized person is actually using the device **104**. In some embodiments, the shared passkey includes an associated timer that identifies the length of time during which the shared passkey is valid. Upon expiration of the passkey timer, a new passkey must be obtained from the remote/payer mobile computing device **102**.

In block **308**, the local/proxy mobile computing device **104** transmits or provides a list of software applications that may be executed on the device **104** and which are authorized to communicate with the remote/payer mobile computing device **102** to request the payment information. By providing a predetermined list of software applications that may request the payment information, the remote/payer mobile computing device **102** may verify that the requesting application is not a malicious, unauthorized application executing on the local/proxy mobile computing device **104** or other device.

In block **310**, the remote/payer mobile computing device **102** generates a private/public encryption key pair and shares the public key with the local/proxy mobile computing device **104**. The encryption keys may be used to encrypt communications between the mobile computing devices **102**, **104**. Any suitable encryption methodology may be used to generate the private/public encryption key pair. For example, in one embodiment, a Rivest, Shamir, and Adleman (RSA) encryption algorithm may be used. The encryp-

tion keys may be generated by and stored in the respective security engines **134**, **154**, which may also be used to encrypt communication between the devices **102**, **104** using the encryption keys.

In block **312**, additional payment parameters may be exchanged between the mobile computing devices **102**, **104**. For example, in some embodiments, a predetermined maximum currency limit may be determined and transmitted to the local mobile computing device **104**. Such currency limits may be embodied as an overall total limit and/or a per-transaction limit. Additionally payment parameters based on, for example, time of purchase, location of purchase, types of items/service purchased, and the like may also be exchanged in block **312**. Such payment parameters may be used by the local/proxy mobile computing device **104** to determine whether the remote/payer mobile computing device **102** may be requested to pay for a particular payment transaction and also provides the user of the remote/payer mobile computing device **102** an amount of control over the types of transactions being paid for by the user of the device **102**.

Referring back to FIG. 2, after a trust relationship has been established between the mobile computing devices **102**, **104**, the local mobile computing device **104** may conduct one or more payment transactions with one or more point-of-sale devices **108** using payment information obtained from the remote mobile computing device **102** in block **204**. In this way, a user of the local mobile computing device **104** may initiate and complete payment transactions for products and/or services with the point-of-sale device **108**, which are paid for by the user of the remote mobile computing device **102** using the payment information provided therefrom. For example, a child may use the local mobile computing device **104** to purchase an amount of gasoline or other product/service, which is paid for by their parent (i.e., the user of the remote mobile computing device **102** on which the payment information is stored).

As illustrated in FIG. 4, one embodiment of a method **400** for conducting a payment transaction begins with block **402** in which the local mobile computing device **104** determines whether the user has initiated a payment transaction with a point-of-sale device **108**. In embodiments wherein the point-of-sale device **108** includes the contactless communication circuitry **160**, the user may initiate the payment transaction by placing the device **104** near the point-of-sale device **108** such that the NFC circuitry **152** and the contactless communication circuitry **160** are able to communicate with each other. However, in other embodiments, the payment transaction may be initiated by other methodologies such as, for example, pressing a key or entering information on a keypad of the point-of-sale device **108**.

In block **404**, the local mobile computing device **104** prompts the user for entry of the passkey. The user may enter the passkey via a keypad or other suitable input device of the mobile computing device **104**. In response, the local mobile computing device **104** compares the entered passkey to the shared passkey received from the remote/payer mobile computing device **102** in block **306** of method **300**. If the passkey is not verified, the method **400** loops back to block **404** wherein the user is again requested to enter a valid passkey. In this way, the identification of the user of the local mobile computing device **104** may be verified.

If the entered passkey is verified in block **404**, the local mobile computing device **104** establishes a secured communication connection with the remote mobile computing device **102** over the network **106** in block **406**. The secured communication connection may be established using, for



example, the unique identification numbers and encryption keys exchanged in blocks 304, 308 of the method 300. For example, the remote mobile computing device 102 may verify the transmitted unique identification number matches the number provided by the local mobile computing device 104 during establishment of the trusted relationship. If such numbers do not match, the remote mobile computing device 102 may terminate the communication connection or take other defensive action.

In block 408, the local mobile computing device 104 receives a payment request from the point-of-sale device 108. The payment request may be in response to previous interaction with the point-of-sale device 108 such as receipt of goods or services provided by the point-of-sale device 108 or a device or entity associated with the device 108. The payment request may include a request for account or other payment information to which the total cost of the product/service is to be billed. In response to receiving the payment request, the local mobile computing device 104 transmits the payment request to the remote mobile computing device 102 in block 410. Such communication may be encrypted or otherwise secured using the shared public encryption key as discussed above.

In block 412, the remote mobile computing device 102 validates the payment request using the data exchanged with the local mobile computing device 104 during establishment of the trust relationship. For example, the remote mobile computing device 102 may be configured to verify the unique identification number (e.g., the IMEI number) of the local mobile computing device 104, verify that the passkey has been entered correctly, and/or verify other parameters established in the method 300. If the payment request is verified, the remote mobile computing device 102 transmits the payment information to the local mobile computing device 104 in block 412. As discussed above, the payment information may be embodied as any type of information required by the point-of-sale device 108 to complete the payment transaction. For example, the payment information may be embodied as account information of the user or owner of the remote/payer mobile computing device 102 such as credit card account information, charge card account information, bank account information, or other account information that may be used to effect payment of a debit.

After the local mobile computing device 104 has received the payment information from the remote mobile computing device 102, the local mobile computing device 104 transmits the payment information to the point-of-sale device 108 in block 414. In response, the point-of-sale device 108 conducts the payment transaction and transmits a payment approval request to the local mobile computing device 104 in block 416. The local mobile computing device 104 forwards the approval request to the remote computing device 102 in block 418.

In block 420, the remote mobile computing device 102 approves the payment based on the approval request. To do so, as discussed above, the remote mobile computing device 102 may verify that the requested currency amount does not exceed a predetermined threshold and/or verify other parameters established in the method 300. If the payment is approved, the remote mobile computing device 102 transmits the a payment approval to the local mobile computing device 104 in block 420.

After the local mobile computing device 104 has received the payment approval from the remote mobile computing device 102, the local mobile computing device 104 transmits the payment approval to the point-of-sale device 108 in block 414. In response, the point-of-sale device 108 com-

pletes the payment transaction and transmits a payment acknowledgement to the local mobile computing device 104 in block 424. The local mobile computing device 104 forwards the payment acknowledgement to the remote computing device 102 in block 426, which may store the payment acknowledgement for future reference. In this way, the local mobile computing device 104 is usable to complete a payment transaction with a point-of-sale device 108 local to the device 104 using payment information stored on and obtained from the remote mobile computing device 102, which may be located remotely from the point-of-sale device 108.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications that come within the spirit of the disclosure are desired to be protected.

The invention claimed is:

1. A method comprising:

establishing a trust relationship between a first mobile phone and a second mobile phone over a Near Field Communication link, by verifying a physical presence of the first mobile phone relative to the second mobile phone;

initiating, by the first mobile phone, a payment transaction with a point-of-sale device;

receiving, with the first mobile phone, a payment request from the point-of-sale device in response to initiating the payment transaction with the point-of-sale device; transmitting, by the first mobile phone and in response to initiating the payment transaction, the payment request received from the point-of-sale device to the second mobile phone over a cellular network, wherein the cellular network is different from the Near Field Communication Link;

receiving, by the first mobile phone, payment information from the second mobile phone in response to the transmittal of the payment request, wherein the payment information includes account information associated with a user of the second mobile phone; and completing, by the first mobile phone, the payment transaction with the point-of-sale device using the payment information received from the second mobile phone.

2. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second mobile phone comprises verifying the physical presence of the first mobile phone relative to the second mobile phone.

3. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second mobile phone comprises exchanging, between the first and second mobile phones, unique identification numbers that identify the corresponding first and second mobile phone.

4. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second mobile phone comprises receiving, with the first mobile phone, a shared passkey from the second mobile phone.

5. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second mobile phone comprises transmitting a list of applications from the first mobile phone to the second mobile phone, the list of applications identifying applications executed on the first mobile phone that are authorized to request payment information from the second mobile phone.

6. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second



## 11

mobile phone comprises receiving, with the first mobile phone, a public key of a public/private key pair from the second mobile phone over the Near Field Communication link.

7. The method of claim 6, wherein transmitting the payment request to the second mobile phone over the cellular network comprises establishing a secured communication connection between the first mobile phone and the second mobile phone using the public key received over the Near Field Communication link.

8. The method of claim 1, wherein establishing a trust relationship between the first mobile phone and the second mobile phone comprises receiving, with the first mobile phone, payment parameters from the second mobile phone, the payment parameters identifying at least one of: a maximum currency amount per transaction and a time period during which the payment information may be obtained from the second mobile phone.

9. One or more non-transitory, machine readable media comprising a plurality of instructions that, when executed by a first mobile computing device, result in the first mobile computing device:

establishing a trust relationship with a second mobile computing device using a Near Field Communication link, by verifying a physical presence of the first mobile phone relative to the second mobile phone;

initiating a payment transaction with a point-of-sale device;

establishing, in response to the initiation of the payment transaction, a secured, wireless communication connection over a cellular network with the second mobile computing device to request payment information therefrom, the cellular network being different from the Near Field Communication link, and the second mobile computing device being remote from the first computing device and the point-of-sale device, wherein the payment information includes account information associated with a user of the second mobile phone; and completing the payment transaction with the point-of-sale device using the payment information received from the first mobile computing device.

10. The one or more non-transitory, machine readable media of claim 9, wherein establishing a trust relationship with the second mobile computing device comprises verifying the physical presence of the second mobile computing device relative to the first mobile computing device using the Near Field Communication link.

11. The one or more non-transitory, machine readable media of claim 9, wherein establishing a trust relationship with the second mobile computing device comprises:

exchanging, with the second mobile computing device, unique identification numbers that identify the corresponding first and second mobile computing devices using the Near Field Communication link;

receiving a shared passkey from the second mobile computing device using the Near Field Communication link; and

receiving a public key of a public/private key pair from the second mobile computing device using the Near Field Communication link.

## 12

12. The one or more non-transitory, machine readable media of claim 9, wherein establishing a trust relationship with the second mobile computing device further comprises receiving payment parameters from the second mobile computing device, the payment parameters identifying a maximum currency amount per transaction.

13. The one or more non-transitory, machine readable media of claim 9, wherein the plurality of instructions further result in the first mobile computing device:

prompting a user for entry of a passkey; and

verifying the entered passkey,

wherein establishing a secured, wireless communication connection over a cellular network with the second mobile computing device comprises establishing a secured, wireless communication connection over a cellular network with the second mobile computing device in response to the passkey being verified.

14. The one or more non-transitory, machine readable media of claim 9, wherein establishing a secured, wireless communication connection over a cellular network with the second mobile computing device comprises:

receiving a payment request from the point-of-sale device;

transmitting the payment request to the second mobile computing device;

receiving encrypted payment information from the second mobile computing device in response to the payment request; and

decrypting the encrypted payment information using a public key of a public/private key pair generated by the second mobile computing device.

15. The method of claim 1, wherein:

establishing the trust relationship between the first mobile phone and the second mobile phone over the Near Field Communication link comprises receiving, with the first mobile phone, payment parameters from the second mobile phone; and

communicating with the second mobile phone over the cellular network comprises communicating with the second mobile phone over the cellular network in response to a determination that the payment transaction has been previously authorized as a function of the payment parameters.

16. The one or more non-transitory, machine readable media of claim 9, wherein:

establishing the trust relationship with the second mobile computing device using the Near Field Communication link comprises receiving payment parameters from the second mobile computing device; and

establishing the secured, wireless communication connection over the cellular network with the second mobile computing device comprises establishing a secured, wireless communication connection over the cellular network with the second mobile computing device in response to a determination that the payment transaction has been previously authorized as a function of the payment parameters.